International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-6, August 2015

Protection Against Power Depletion Attack in WLAN

Sruthin R V, Jayasudha J S

Abstract— Power depletion attacks in internet are mainly affecting the Wireless LANs, since they are working on battery power which is the main resource of interest. The attack is performed by generating and routing unnecessarily packets in the network there by consuming the nodes battery power. The vulnerable packet movement in the network is identified using entropy estimation model which is different from the packet marking scheme. The vulnerable nodes in the network are identified by a packet routing scheme, which improves efficiency while using the entropy estimation model. The system is scanned for possible attack virus presence in the host node, which in turn spread the virus to the vulnerable nodes in the network. A novel hybrid method is proposed by combining three existing method which is used to protect the WLANs from power depletion attacks.

Index Terms— Entropy value, bounce packet, vulnerable host.

I. INTRODUCTION

WLANs have a large application in areas where no fixed communication and computational resources are available. Thus they are used in remote areas for providing communication and computational resource. These are used by researchers in remote area, for first responders in disaster stood areas and also for troop deployment by military. In these areas electric power is a scare resource which is required for making the whole network alive. The WLANs are vulnerable to DoS attacks [1] and a number of defence mechanism [1], [2] are already proposed. These WLANs are also vulnerable to permanent denial of service attack which is carried out by completely depleting the nodes battery power. Thus the whole network goes to dead state, even if a part of the network is dead then the communication between the team members is broken and the benefit of the network will be negative.

The attack is performed in such a way that the nodes in the network are made active and make them process the packets that are not to be processed by them in the network. Thus the nodes are made to consume more energy from the network to do no useful work and thus the energy is drained faster from the network. This makes the network dead, far earlier than expected. Since it is a hard and time consuming task to restore the energy in remote places, it is necessary to control these issues. A packet marking schemes is introduced to protect the network from these power depletion attack but they need the routers to perform extra computational work and it modify the packet header which sometimes will causes in the loss or damage of packet. This will also increases the length of the packet. When this method is implemented in large network, the size of packet will increase accordingly and eventually results in a negative effect to the method by utilizing more energy.

The attack in the network is identified by using an entropy estimation method. The entropy growth rate indicates that whether there is an attack in the network or not. The packet in the network is classified according to the protocol type and the destination port number. The variation in the flow rates for each class of packet is analysed to calculate the entropy value at each time interval. To improve the efficiency in identifying the attacking node, a packet routing mechanism is used. Packets are sent to all active nodes in the network and the number of bounce packets for each connection is calculated to identify the vulnerable node. The attacking virus will be spreading in the network by replicating itself to the vulnerable host in the network. The system is scanned for possible virus behaviour and protection is to be taken to avoid the spreading of the virus in the network. The above mechanism will work together to avoid the power depletion attack in the network.

II. RELATED WORK

There is a large number of power draining attacks and many defence mechanism against them are introduced but they are not suitable to give protection from all types of attacks. The '*sleep deprivation torture*' attack is the oldest attack that prevents the nodes from entering a low power sleep cycle [3]. Thus the nodes consume more energy and eventually drain the power completely. Attacks by using malicious loops and its prevention methods are briefly mentioned in [4], [5] but they focus only in these type of attacks. Long term denial of service attack is described in [11], [12], [13].

Many works are done on minimum energy routing in WLANs which is beneficial for networks where energy is a constrain. They aim at reducing the energy for receiving and transmission of packets since they are the most energy consuming actions in a network. Sheetalkumar Doshi *et al.* proposed the '*An on demand minimum energy routing protocol for a wireless ad hoc network*' [6] which reduces the energy requirement for transferring a packet from source to destination by increasing the number of intermediate nodes which in turn reduces the distance between the intermediate nodes. Jae-Hwan Chang *et al*. proposed which also aim at reducing the transmission cost for packets through reducing the distance between intermediate nodes [7]. The attack will even occur in this reduced transmission cost scenario since they work on cooperative nodes and not on malicious.

Manuscript published on 30 August 2015.
* Correspondence Author (s)
Sruthin R V*, Department of Computer Science, University of Kerala/ SCT College of Engineering, Trivandrum, India.
Dr. Jayasudha J S, Department of Computer Science, University of Kerala, SCT College of Engineering, Trivandrum, India.

Research works are done on the basis of information theory. Lee and Xiang examined several information theoretic methods for intrusion detection [8], [17]. They use entropy and conditional entropy model to partition data and identifying the parameters for intrusion detection model. Here we need to analyse the anomalies in network traffic which causes fluctuation in network traffic rate or contents. Staniford *et al.* proposes a information theoretic method to detect anomalous port scans [9]. An entropy based approach for detecting anomalies in network traffic is examined in [14], [10]. It is possible to identify the anomaly that changes the traffic rate abruptly or slowly. Memory and computational time required are directly proportional to the traffic rate. Secure routing methods are proposed in [15], [16] but attacks are protocol independent and cannot be prevented.

III. Protection against Power Depletion Attack

The power depletion attack in networks is characterised by large fluctuation in data flow statistics in the network. The attack is thus identified by analysing the data flow in the network. Here an entropy estimation model is used to analysis the packet movement in the network, where the packets are classified according to the header details like the protocol used and the port number to which the packet is sent. The performance of analysing the power depletion attack by entropy estimation model is improved by a packet routing scheme. This packet routing scheme is used to identify the attacking nodes by using the time delay in transmission of packets and the rate of bounce packet in the network. A file scan method is used to scan the system for possible virus behaviour since the host node must not be an attacker otherwise it will be a contradiction. The techniques used are explained below.

A. *Entropy Estimation Model*

An entropy estimation model is used to analyse the changes in the network traffic. Here the packets in the network are classified in to groups according to their protocol type and port number. The packets are initially classified in to TCP and UDP packets, which are then again classified in to SYN and RST packets. For each set of classifications the packets are again divided according to the port number. The port number is generally divided into three class they are well-known ports (0 - 1023), registered ports (1024 - 49151) and dynamic or private ports (49152 - 65535). The ports in the well-known port groups are grouped to a set of 10 ports with an exception for port 80 since more traffic will be for that port. Thus a new 104 classes of packets are created. The registered ports are grouped into a set of 100 ports with an exception of only 28 ports in the last class. Here a group of 482 additional classes are created. The private port set is made as a single group. Thus the total classes according to port number is 587 and the total class of packets in the network is 2348 since there is a two dimensional classification in protocol layer. The packet monitoring in networks is shown in figure 1.

Maximum Entropy estimation is used for obtaining a parametric probability distribution model for the packet class in the network. Maximum Entropy estimation produces a model with the most 'uniform' distribution among all the distributions satisfying the given constraints [10], [14]. The mathematical representation of entropy for the distribution P is given in equation 1.

$$H(P) = -\sum_{\omega \in \Omega} P(\omega) \log P(\omega) \quad (1)$$

Here Ω be the set of packet classes defined above. The sequence of packets for the analysis be S = {x_1, x_2,... x_n}, and the empirical distribution P over Ω is given in equation 2.

$$P'(\omega) = \frac{\sum \mathbf{I}(x_i \in \omega)}{n} \quad (2)$$

Where **I**(*X*) is an indicator function that takes the value 1 if *X* is true and 0 if *X* is false.

The analysis has a set of feature function $F = \{f_i\}$ and f_i be an indicator function. While using Maximum Entropy model, it is necessary to have a density model *P* that satisfies the condition $E_p(f_i) = E_{P'}(f_i)$ for all $f_i \in F$. It is proved that the Maximum Entropy model is (a) unique and (b) the same as the generalised Gibbs distribution [11] given in equation 3.

$$P(\omega) = \frac{1}{Z} \exp\left(\sum_i \lambda_i f_i(\omega)\right) \quad (3)$$

For each feature function f_i we have a corresponding weight, λ_i to it. Z is normalization constant to ensure the sum of the probabilities over Ω is 1.

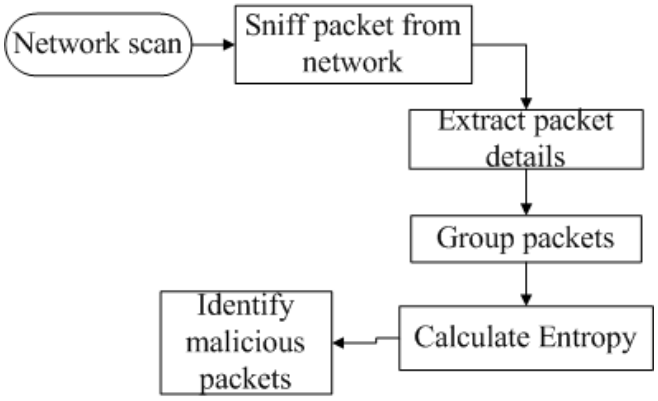

Figure 1. Packet monitoring in network

B. *Packet Routing Method*

The main objective of packet routing is to point out the suspicious node in the network. Here the entire active node in the network is to be identified. The nodes that are not receiving or acknowledging the packets sent by another node are suspicious nodes since somehow the packet and the acknowledgment to those nodes are rerouted, modified or dropped in the transit to the destination. These anomalies are identified according to the increasing number of bounce packets and the time delay in sending packets as shown in figure 2. The packets that reach the source without reaching the destination are called bounce packets. As the number of bounce packets increases the time delay will also increase since the source is waiting more time for the acknowledgment to come.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

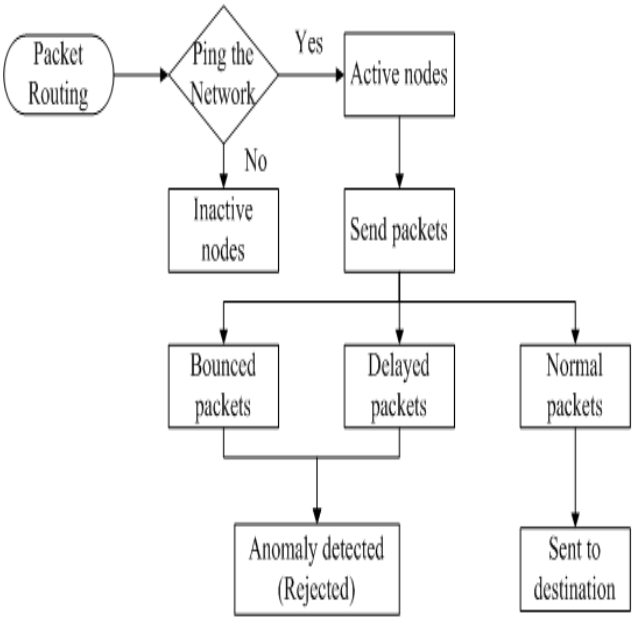

Figure 2. Packet routing

In this method the network is scanned to obtain all the active packets in the network. Once the active nodes are identified, they are arranged in a plane in a random manner with coordinate value. The nodes are arranged in a connected manner in the plane. Initially an equal energy value is assigned to all the nodes. The energy is directly proportional to time and its consumption is calculated according to the time for which the node is sending or receiving packet. After energy is assigned to all nodes in the network, the nodes starts transmitting packets to other nodes in the network and also listen to the acknowledgment and bounce packet from the network. The bounce packet for each node is counter separately along with the time delay in transmitting packet. The node with more number of bounce packets is suspicious to power depletion attack. The anomaly is detected according to the rate of delay in transmitting packet and to the rate of bounce packet from that node.

C. System Scan

The attacking software will have the behaviour of a virus or worm. They will spread to other nodes in the network. The attack is spreading in such a way that the infected node will check for vulnerable systems like the one having outdated antivirus or no antivirus, flaws in protocols etc. and those nodes will be infected thereafter. The attack will be more if the number of infected nodes in the network is large. So we need to verify whether the node is infected or not.

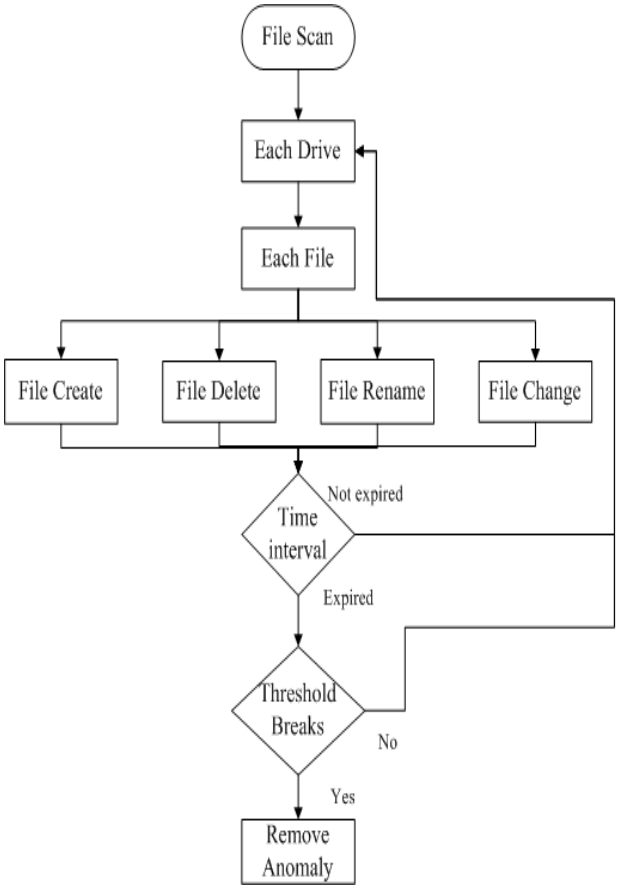

Figure 3. System scan

To identify the presence of virus in the node, we are scanning the system for possible virus behaviour like anomalous file change, create, delete and file rename as shown in figure 3. The system is scanned in each drive and all files are verified. A file is examined for any of the four actions has happened or not. The system is scanned and at each time interval the numbers of files that are changed, created, deleted or renamed are calculated. If any of the actions has a value greater than a normal count then the time and files that contribute to the abnormal change is reported. The reports are verified and if the changes are made by unknown procedures then necessary protection schemes are to be introduced.

IV. PERFORMANCE ANALYSIS

The performance analysis for detecting the power depletion attack in WLAN is carried at different networks under both attack and non attack conditions. The entropy value is calculated for each network, for a time period at a fixed time interval, both under the attack and non attack scenarios. The mean variance entropy curve for a network under non attack condition is a parabolic curve with the mean entropy value decreasing for a fixed constant. Under attack condition the mean entropy curve shows difference in the curve behaviour with pikes in the graph. The pikes in the curve are created due to the abrupt changes in the packet flow rate.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

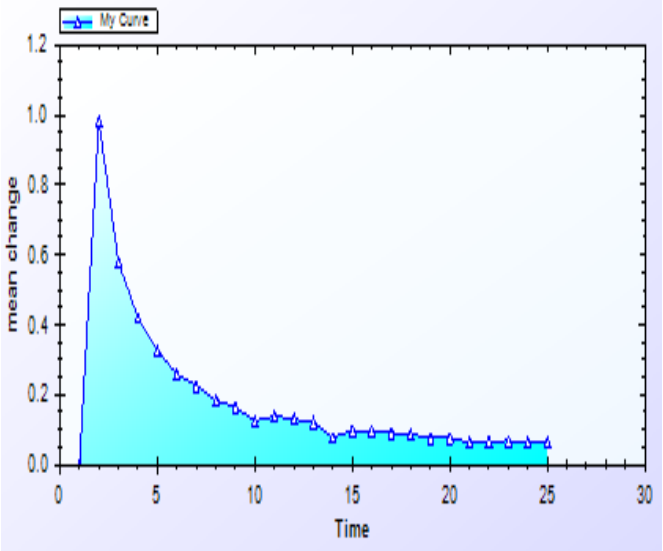

Figure 4. Mean Variance Entropy curve for non attack condition

The figure 4 shows the mean variance entropy curve under non attack scenario, where the graph starts from a maximum value of one and reduces parabolic to a lower value as time expands. The figure 5 shows the mean variance entropy curve under attack scenario, here there are distortions in the curve created for the flow.

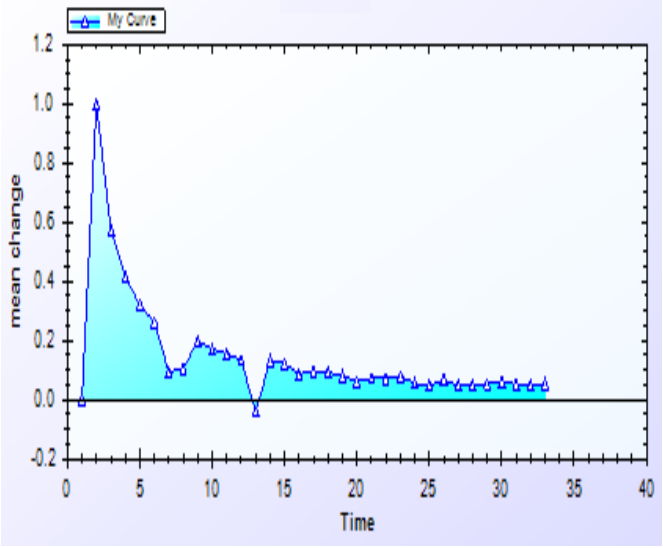

Figure 5. Mean Variance Entropy curve for attack condition

V. CONCLUSION AND FUTURE WORKS

In this paper, a hybrid method is proposed for protecting the system from power depletion attack. This paper also includes the different possible ways of power depletion attacks and defence mechanisms. It is necessary to analyse the network for abrupt changes in the flow statistics in the network which in turn consumes more energy and makes the nodes drain its energy faster. The anomalies in the network traffic are calculated by using the entropy estimation model, which is a better method to identify the attacking nodes in a smaller network. In order to identify the attacking node in a larger network a packet routing scheme is used in addition to entropy estimation model. The packet routing model uses the delay time and also the number of bounce packets to identify the suspicious nodes in the network. Thus the coexistence of both the entropy estimation model and the packet routing model is necessary for correctly identifying the attacking nodes in the network. The host system must not be a host for spreading the attacking virus, thus to identify the presence of virus in the system, a file scan is done to identify the possible virus behaviour in the system. The file scan is performed by analysing the file creation, deletion, change and rename rates in the network. Thus the proposed hybrid method is used to secure the network from power depletion attacks.

In larger networks a routing mechanism is used to identify the attacker nodes in the network, but it creates more traffic in the network and drains more energy in the network. Thus at some critical conditions this scan itself act as an attack. Thus the efficiency of entropy estimation model can be improved to avoid the routing method, which can be done as a future enhancement.

REFERENCES

1. Anthony D. Wood and John A. Stankovic, " Denial of service in sensor networks", IEE Computer Society, Computer, vol. 35, no. 10., pp. 54-62, Oct 2002.
2. John Bellardo and Stefan Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions", SSYM'03 Proceedings of the 12th conference on USENIX Security Symposium, vol. 12, pp 2-2, Aug. 2003.
3. Frank Stajano and Ross Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks", International workshop on security protocols, vol. 7, pp. 172-182, April 1999.
4. Haowen Chan and Adrian Perrig," Security and privacy in sensor networks", IEE Computer Society, Computer, vol. 36, no. 10. Oct 2003.
5. Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, "Secure sensor network routing: A clean-slate approach", ACM CoNEXT conference, 2006.
6. Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, "An on demand minimum energy routing protocol for a wireless adhoc network", ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 3, 2002.
7. Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking, vol.12, no. 4, 2004.
8. Wenke Lee and Dong Xiang, " Information-theoretic measures for anomaly detection", In Proceedings of the IEEE Symposium on Security and Privacy , IEEE Computer Society, pp. 130. 2001.
9. Staniford, Hoagland and Mcalerney. "Practical automated detection of stealthy portscans". Proceedings of the IDS Workshop of the 7th Computer and Communications Security Conference , 2000.
10. Yu Gu, Andrew McCallum, Don Towsley. "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation". Proceedings of the 5th ACM SIGCOMM conference on internet measurement, page 32-32, 2005.
11. Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak and JenniferRexford," Path-quality monitoring in the presence of adversaries", Proceedings of the ACM SIGMETRICS international conference on Measurement and modeling of computer systems, vol. 36, no. 1, pp. 193-204, 2008.
12. Mina Guirguis, Azer Bestavros, Ibrahim Matta and Yuting Zhang, "Reduction of quality (RoQ) attacks on Internet end-systems", Infocom'05: The IEEE International Conference on Computer Communication, vol. 2, pp. 1362-1372, 2005.
13. Yu-Kwong Kwok, Rohit Tripathi, Yu Chen, and Kai Hwang, 'HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks", Networking and mobile computing, 2005.
14. Mr.T.Bharath Manohar, Mrs.E.V.N.Jyothi, Mrs.B.Rajani, Mr.I.Rajesh Kumar, "A Novel Entropy Based Detection of DDoS Attacks", International Journal of Emerging Trends & Technology in Computer Science, Volume 1, Issue 2, July – August 2012.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

15. Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks", INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, vol. 3, pp. 1976-1986, April 2003.
16. Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", WiSe Proceedings of the 2nd ACM workshop on Wireless security, pp. 30-40, September 2003.
17. Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks". IEEE Transactions on Mobile Computing, volume 12, issue 2, pp. 318-332, 2012.

Sruthin R V is currently doing his MTech in Computer Science and Engineering at Sree Chitra Thirunal College of Engineering under Kerala University, Trivandrum, Kerala, India. Sruthin received his B Tech Degree in Computer Science and Engineering from College of Engineering, Perumon under CUSAT, Kerala, India in 2012. He concentrates mainly on security, wireless network, distributed computing and cloud computing.

Dr. Jayasudha J S is working as professor and head of the department at the department of computer science and engineering, Sree Chitra Thirunal College of Engineering, Trivandrum, Kerala. She did her B. E. degree from Madurai Kamaraj University and M.E. degree from National Institute of Technology, Trichy and doctorate degree from University of Kerala. Her Ph.D. thesis title is "Web caching and Pre-fetching techniques for Web traffic/Latency reduction". She is recognized as approved research guide for PhD works in Computer Science and guiding Ph.D. students in Manonmaniam Sundaranar University and Noorul Islam University. Now she is also doing research in Computer Networks. She published her research works in many national and international conferences and journals. She has 19 years of teaching experience and organized many community development programs, short term courses and conferences.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)